日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年 ４月２８日

出 願 番 号
Application Number: 平成１１年特許願第１２１２００号

出 願 人
Applicant (s): カシオ計算機株式会社

２０００年 ２月２５日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆 彦

出証番号 出証特２０００－３００９９７２

【書類名】　特許願

【整理番号】　98-2289-00

【あて先】　特許庁長官殿

【国際特許分類】　G06F 17/00

【発明者】

【住所又は居所】　東京都羽村市栄町３丁目２番１号
カシオ計算機株式会社羽村技術センター内

【氏名】　森川　重則

【発明者】

【住所又は居所】　東京都羽村市栄町３丁目２番１号
カシオ計算機株式会社羽村技術センター内

【氏名】　井口　敏之

【発明者】

【住所又は居所】　東京都羽村市栄町３丁目２番１号
カシオ計算機株式会社羽村技術センター内

【氏名】　大塚　基

【特許出願人】

【識別番号】　000001443

【氏名又は名称】　カシオ計算機株式会社

【代理人】

【識別番号】　100074985

【弁理士】

【氏名又は名称】　杉村　次郎

【手数料の表示】

【予納台帳番号】　023180

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

出証特２０００－３００９９７２

【物件名】　　要約書　1

【包括委任状番号】　9109737

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　データ処理装置およびそのプログラム記録媒体

【特許請求の範囲】

【請求項１】

アプリケーションソフト／データが格納されている持ち運び自在な記録媒体がセットされている状態でこの記録媒体内のアプリケーションソフト／データをアクセスしてデータ処理を行うデータ処理装置において、

前記記録媒体内のアプリケーションソフト／データをアクセスする際に、データ処理装置固有の識別情報がアクセス制御情報としてその記録媒体内に予め格納されている場合に、この記録媒体から前記識別情報を読み込む読込手段と、

この読込手段によって読み込まれた識別情報と予め設定されている自己の識別情報とを比較する比較手段と、

この比較手段による比較結果に基づいて前記記録媒体内のアプリケーションソフト／データに対するアクセス可否を決定するアクセス制御手段とを具備したことを特徴とするデータ処理装置。

【請求項２】

同一グループに属する複数台のデータ処理装置に対応してその装置固有の識別情報が複数格納されているグループ対応の記録媒体をアクセスする場合に、

前記アクセス制御手段は前記記録媒体から読み込んだ複数の識別情報の中に、予め設定されている自己の識別情報が含まれているか否かに基づいて当該記録媒体内のアプリケーションソフト／データに対するアクセス可否を決定するようにしたことを特徴とする請求項１記載のデータ処理装置。

【請求項３】

前記記録媒体内に複数のアプリケーションソフト／データが格納されていると共に、個々のアプリケーションソフト／データに対応付けてデータ処理装置固有の識別情報が格納されている場合に、

前記読込手段はアクセス対象として指定されたアプリケーションソフト／データに対応する識別情報を読み込み、

前記アクセス制御手段は前記記録媒体から読み込まれた識別情報と予め設定さ

れている自己の識別情報とを比較することによりアプリケーションソフト／データ毎にアクセス可否を決定するようにしたことを特徴とする請求項１記載のデータ処理装置。

【請求項４】

持ち運び自在な記録媒体にアプリケーションソフト／データを書き込むことにより、この記録媒体を介して各端末側にアプリケーションソフト／データを配布するデータ処理装置において、

アプリケーションソフト／データをアクセスすることが許可／禁止された端末に対して予め割り当てられている端末固有の識別情報をアクセス制御情報として取得する取得手段と、

この取得手段によって得られた端末識別情報をアプリケーションソフト／データに対応付けてその記録媒体内に書き込む書込手段とを具備したことを特徴とするデータ処理装置。

【請求項５】

個々のアプリケーションソフト／データ毎にそのアクセスを許可／禁止する端末を定義する定義情報を参照し、前記書込手段は端末対応の記録媒体毎に書き込み対象としてのアプリケーションソフト／データを特定すると共に、特定されたアプリケーションソフト／データをその端末識別情報と共に記録媒体内に書き込むようにしたことを特徴とする請求項４記載のデータ処理装置。

【請求項６】

同一グループに属する複数の端末へ前記記録媒体を介してアプリケーションソフト／データを配布する際に、前記取得手段は、そのグループに属する各端末固有の識別情報を複数取得し、

前記書込手段はこの取得手段によって得られた同一グループに属する複数の端末識別情報をアプリケーションソフト／データと共に書き込むようにしたことを特徴とする請求項４記載のデータ処理装置。

【請求項７】

端末装置との間でネットワークを介してデータ通信を行うデータ処理装置において、

各アプリケーションソフト／データに対応して端末識別情報をアクセス制限情報として記憶するアクセス制限情報記憶手段と、

いずれかの端末装置からアプリケーションソフト／データに対するアクセス要求があった際に、要求元の端末装置から送信されて来た端末識別情報とアプリケーションソフト／データに対応する端末識別情報とを比較する比較手段と、

この比較手段による比較結果に基づいてアプリケーションソフト／データに対するアクセス可否を決定するアクセス制御手段とを具備したことを特徴とするデータ処理装置。

【請求項８】

コンピュータによって読み取られるプログラムコードを有する記録媒体であって、

アプリケーションソフト／データが格納されている持ち運び自在な記録媒体がセットされている状態での記録媒体内のアプリケーションソフト／データをアクセスする際に、この記録媒体からデータ処理装置固有の識別情報を読み込む機能と、

この識別情報と予め設定されている自己の識別情報とを比較する機能と、

この比較結果に基づいて前記記録媒体内のアプリケーションソフト／データに対するアクセス可否を決定する機能を実現するためのプログラムコードを有する記録媒体。

【請求項９】

コンピュータによって読み取られるプログラムコードを有する記録媒体であって、

アプリケーションソフト／データをアクセスすることが許可／禁止されている端末に対して予め割り当てられている端末固有の識別情報をアクセス制御情報として取得する機能と、

このアプリケーションソフト／データに対応付けてその記録媒体内に書き込む機能を実現するためのプログラムコードを有する記録媒体。

【請求項１０】

コンピュータによって読み取られるプログラムコードを有する記録媒体であっ

て、

いずれかの端末装置からネットワークを介してアプリケーションソフト／データに対するアクセス要求があった際に、要求元の端末装置から送信されて来た端末識別情報と、アプリケーションソフト／データに対応する端末識別情報とを比較する機能と、

この比較結果に応じてアプリケーションソフト／データに対するアクセス可否を決定する機能を実現するためのプログラムコードを有する記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、アプリケーションソフト／データのアクセスを制御するデータ処理装置およびそのプログラム記録媒体に関する。

【０００２】

【従来の技術】

一般に、アプリケーションソフトはフロッピーディスクやコンパクトディスク等の記録媒体を介してパーソナルコンピュータ（パソコン）に別途提供され、これをパソコン上でインストールすることにより起動される。この場合、ソフトメーカはアプリケーションソフトにユニークなプロダクト番号を付けて出荷する。このソフトをユーザがパソコン上でインストールして動作させる場合、許可キーとしてこのプロダクト番号をキーボードから入力するようにしている。

一方、複数台の端末装置がネットワークを介して通信接続されて成るオンライン型のクライアント・サーバシステムにおいて、各クライアント端末はネットワークを経由してアプリケーションソフトを入手するようにしている。この場合、クライアント端末からサーバへアプリケーションソフトのコピー転送を要求するが、その際、ユーザは自己のＩＤとパスワードを入力するようにしている。

【０００３】

【発明が解決しようとする課題】

しかしながら、記憶媒体を介して提供されるアプリケーションソフトは、そのプロダクト番号さえ分かれば、複数台のパソコンに何回もインストールすること

ができ、不法なコピー複製が可能となる。このようなコピー複製を禁止するためには、一旦、アプリケーションソフトをインストールしたらその記憶媒体の内容を全てクリアする必要がある。しかしながら、記憶媒体の内容を全てクリアしてしまうと、その後、障害が発生し、再度インストールする必要が生じたときには、それに対応することができなくなり、また記憶媒体の内容をその都度クリアするという面倒な作業を強要することにもなる。

また、ネットワーク経由でクライアント端末からサーバへアクセスする場合、ユーザＩＤとパスワードとを知っていれば、誰でもどの端末からでもアプリケーションソフトをアクセスすることができ、不正アクセスの可能性がある。

このことはアプリケーションソフトに限らず、機密性の高い重要データを記憶媒体を介して提供する場合やネットワーク経由で提供する場合においても同様であり、セキュリティ維持の点で問題があった。

第１の発明の課題は、アプリケーションソフト／データが格納されている記録媒体をアクセスしてデータ処理を行うデータ処理装置において、特定のデータ処理装置に対してのみ記録媒体内のアプリケーションソフト／データのアクセスを許可することで、装置毎のアクセス制御が可能となり、セキュリティ維持と共にアクセス権限を有しない他の装置による不法なコピー複製を効果的に禁止できるようにすることである。

第２の発明の課題は、アプリケーションソフト／データを記録媒体に書き込んで各端末に配布するデータ処理装置において、特定端末に対してのみアプリケーションソフト／データのアクセスを許可／禁止するための書き込みを行うことで、端末毎のアクセス制御が可能となりセキュリティ維持と共に、アクセス権限を有しない他の端末による不法なコピー複製を効果的に禁止できるようにすることである。

第３の発明の課題は、端末装置との間でネットワークを介してデータ通信を行うデータ処理装置において、特定端末に対してのみアプリケーションソフト／データのアクセスを許可することで、不法なアプリケーションソフト／データのダウンロードを禁止し、そのセキュリティを維持できるようにすることである。

【０００４】

【課題を解決するための手段】

この発明の手段は次の通りである。

請求項１記載の発明（第１の発明）は、アプリケーションソフト／データが格納されている持ち運び自在な記録媒体がセットされている状態でこの記録媒体内のアプリケーションソフト／データをアクセスしてデータ処理を行うデータ処理装置において、前記記録媒体内のアプリケーションソフト／データをアクセスする際に、データ処理装置固有の識別情報がアクセス制御情報としてその記録媒体内に予め格納されている場合に、この記録媒体から前記識別情報を読み込む読込手段と、この読込手段によって読み込まれた識別情報と予め設定されている自己の識別情報とを比較する比較手段と、この比較手段による比較結果に基づいて前記記録媒体内のアプリケーションソフト／データに対するアクセス可否を決定するアクセス制御手段とを具備するものである。

なお、同一グループに属する複数台のデータ処理装置に対応してその装置固有の識別情報が複数格納されているグループ対応の記録媒体をアクセスする場合に、前記アクセス制御手段は前記記録媒体から読み込んだ複数の識別情報の中に、予め設定されている自己の識別情報が含まれているか否かに基づいて当該記録媒体内のアプリケーションソフト／データに対するアクセス可否を決定するようにしてもよい。

また、前記記録媒体内に複数のアプリケーションソフト／データが格納されていると共に、個々のアプリケーションソフト／データに対応付けてデータ処理装置固有の識別情報が格納されている場合に、前記読込手段はアクセス対象として指定されたアプリケーションソフト／データに対応する識別情報を読み込み、前記アクセス制御手段は前記記録媒体から読み込まれた識別情報と予め設定されている自己の識別情報とを比較することによりアプリケーションソフト／データ毎にアクセス可否を決定するようにしてもよい。

請求項１記載の発明においては、アプリケーションソフト／データと共にデータ処理装置固有の識別情報（例えば、端末ＩＤ）が格納されている記録媒体をアクセスする際に、この記録媒体から識別情報を読み込み、この識別情報と予め設定されている自己の識別情報とを比較し、この比較結果に基づいて記録媒体内の

アプリケーションソフト／データに対するアクセス可否を決定する。

したがって、アプリケーションソフト／データが格納されている記録媒体をアクセスしてデータ処理を行うデータ処理装置において、特定のデータ処理装置に対してのみ記録媒体内のアプリケーションソフト／データのアクセスを許可することで、装置毎のアクセス制御が可能となり、セキュリティ維持と共にアクセス権限を有しない他の装置による不法なコピー複製を効果的に禁止することができる。

【０００５】

請求項４記載の発明（第２の発明）は、持ち運び自在な記録媒体にアプリケーションソフト／データを書き込むことにより、この記録媒体を介して各端末側にアプリケーションソフト／データを配布するデータ処理装置において、アプリケーションソフト／データをアクセスすることが許可／禁止された端末に対して予め割り当てられている端末固有の識別情報をアクセス制御情報として取得する取得手段と、この取得手段によって得られた端末識別情報をアプリケーションソフト／データに対応付けてその記録媒体内に書き込む書込手段とを具備するものである。

なお、個々のアプリケーションソフト／データ毎にそのアクセスを許可／禁止する端末を定義する定義情報を参照し、前記書込手段は端末対応の記録媒体毎に書き込み対象としてのアプリケーションソフト／データを特定すると共に、特定されたアプリケーションソフト／データをその端末識別情報と共に記録媒体内に書き込むようにしてもよい。

また、同一グループに属する複数の端末へ前記記録媒体を介してアプリケーションソフト／データを配布する際に、前記取得手段は、そのグループに属する各端末固有の識別情報を複数取得し、前記書込手段はこの取得手段によって得られた同一グループに属する複数の端末識別情報をアプリケーションソフト／データと共に書き込むようにしてもよい。

請求項４記載の発明においては、アプリケーションソフト／データをアクセスすることが許可／禁止された端末に対して予め割り当てられている端末固有の識別情報を取得し、この識別情報をアプリケーションソフト／データに対応付けて

その記録媒体内に書き込む。

したがって、アプリケーションソフト／データを記録媒体に書き込んで各端末に配布するデータ処理装置において、特定端末に対してのみアプリケーションソフト／データのアクセスを許可／禁止するための書き込みを行うことで、端末毎のアクセス制御が可能となりセキュリティ維持と共に、アクセス権限を有しない他の端末による不法なコピー複製を効果的に禁止することができる。

【０００６】

請求項７記載の発明（第３の発明）は端末装置との間でネットワークを介してデータ通信を行うデータ処理装置において、各アプリケーションソフト／データに対応して端末識別情報をアクセス制限情報として記憶するアクセス制限情報記憶手段と、いずれかの端末装置からアプリケーションソフト／データに対するアクセス要求があった際に、要求元の端末装置から送信されて来た端末識別情報とアプリケーションソフト／データに対応する端末識別情報とを比較する比較手段と、この比較手段による比較結果に基づいてアプリケーションソフト／データに対するアクセス可否を決定するアクセス制御手段とを具備するものである。

請求項７記載の発明においては、いずれかの端末装置からアプリケーションソフト／データに対するアクセス要求があった際に、要求元の端末装置から送信されて来る端末識別情報と、アプリケーションソフト／データに対応する端末識別情報とを比較し、その比較結果に応じてアプリケーションソフト／データに対するアクセス可否を決定する。

したがって、端末装置との間でネットワークを介してデータ通信を行うデータ処理装置において、特定端末に対してのみアプリケーションソフト／データのアクセスを許可することで、不法なアプリケーションソフト／データのダウンロードを禁止し、そのセキュリティを維持することができる。

【０００７】

【発明の実施の形態】

（第１実施形態）

以下、図１～図７を参照してこの発明の第１実施形態を説明する。

図１はオフライン型のクライアント・サーバシステムを示したシステム構成図

である。すなわち、会社組織において、会社内に設置されているサーバコンピュータ１と、各営業担当者が持参するモバイル型のクライアント端末（携帯端末）２とを有し、各営業担当者は外出先で可搬型記録媒体３内のアプリケーションソフト／データベースをアクセスしながら営業活動を行い、そして、一日の営業終了時に、端末本体から可搬型記録媒体３を抜き取り、サーバコンピュータ１のカードリーダ／ライタ４にセットすると、サーバコンピュータ１はカードリーダ／ライタ４を介してＣＦカード３内の営業記録を収集処理するオフライン型のシステムである。ここで、可搬型の記録媒体３は取り外し可能なコンパクトフラッシュカードであり、以下、ＣＦカード３と称する。サーバコンピュータ１に付属されているカードリーダ／ライタ４は、各クライアント端末対応のＣＦカード３が複数枚同時にセット可能なもので、各ＣＦカード３を順次アクセスしてデータの読み込み／書き込みを行う。なお、図中、ＣＦカード３に付した「＃１」、「＃２」、「＃３」は、端末名称｛Ａ１」、「Ｂ１」、「Ｃ１」で示される携帯端末２に対応付けられ、携帯端末２と１：１に対応付けられた端末対応のＣＦカード３であることを示している。なお、この実施形態においては端末対応のＣＦカード３の他、後述する端末グループ対応のＣＦカード３も存在するが、図１の例では端末対応のＣＦカード３のみを示している。サーバコンピュータ１はこのＣＦカード３を介して携帯端末２側へアプリケーションソフト（ＡＰソフト）／データベースを配布する。すなわち、サーバコンピュータ１はＡＰソフト格納部５、データベース格納部６の内容を読み出してカードリーダ／ライタ４に与え、それにセットされている各ＣＦカード３にＡＰソフト／データベースを書き込むが、その際、サーバコンピュータ１は端末登録テーブル７、アプリ・データ設定テーブル８を参照してどの端末に何を書き込むかを判別し、ＡＰソフト／データベースを特定して該当するＣＦカード３内に書き込むと共に端末識別情報（端末ＩＤ）をＡＰソフト／データベースに対するアクセス制御情報としてＣＦカード３内に書き込む。

【０００８】

図２はＣＦカード３に格納されているデータを示したもので、（Ａ）は端末対応のＣＦカード３の内容を示している。この端末対応のＣＦカード３は、それを

識別するための固有の媒体番号と、このカードを専用する携帯端末２を識別するための固有の端末ＩＤと、ＡＰソフト、データベースとを記憶する構成で、この例では媒体番号「Ｍ０１」、端末ＩＤ「ＩＤ１１」、ＡＰソフト「α１」、データベース「Ｄ１」が格納されている。ここで、ＡＰソフト／データベースと端末ＩＤとの対応関係は、そのアクセスを許可する端末を定義するもので、端末対応のＣＦカード３には１種類の端末ＩＤが設定されている。

また、図２（Ｂ）は端末グループＡ対応のＣＦカード３の内容を示し、図３に示すように「＃１Ａ」を付した各ＣＦカード３は、端末名称が「Ａ１」、「Ａ２」、「Ａ３」である各携帯端末２が属する端末グループＡ対応の記憶媒体で、そのグループ対応の各ＣＦカード３には、「媒体番号」の他、各種のＡＰソフト／データベース毎に１または２以上の端末ＩＤが格納されており、「媒体番号」を除く他のデータは、そのグループ内において同一内容となっている。なお、図２（Ａ）で示した端末ＩＤは図３に示すように端末グループＡに属する各携帯端末２毎に割り当てられた固有の端末識別情報であり、ＡＰソフト／データベースと端末ＩＤとの対応関係は、端末対応の場合と同様に、そのアクセスを許可する端末を定義する。また、図２（Ｃ）は端末グループＢ対応のＣＦカード３の内容を示し、そのデータ構造は図２（Ｂ）で示した端末グループＡの場合と同様であるため、その説明は省略するが、端末グループＢ対応の各ＣＦカード３内に設定された端末ＩＤは、図３に示すように端末グループＢに属する各携帯端末２毎に割り当てられた端末識別情報である。

【０００９】

図４はサーバコンピュータ１側に設けられている端末登録テーブル７、アプリ・データ設定テーブル８、グループ登録テーブル９のデータ構造を示したもので、図４（Ａ）は端末登録テーブル７の内容を示している。この端末登録テーブル７はアプリ・データ設定テーブル８を作成する際や端末対応のＣＦカード３にＡＰソフト／データベースを書き込む際に参照されるもので、「端末名称」、「端末ＩＤ」、「媒体番号」とを対応付けた構成で、システム構築時や新たな媒体を追加採用するとき等にその設定登録が行われる。アプリ・データ設定テーブル８は図４（Ｂ）に示すように、ＡＰソフト／データベース毎に、そのソフト名／デ

ータベース名に対応付けて、１または２以上の端末ＩＤを記憶する構成で、サーバコンピュータ１はＣＦカード３にＡＰソフト／データベースを書き込む際に参照される。

【００１０】

図５は、サーバコンピュータ１、携帯端末２の全体構成を示したブロック図である。なお、サーバコンピュータ１、携帯端末２の構成要素は基本的に同一であるため、図中１１～１６はサーバコンピュータ１に対応する構成要素とし、図中２１～２６は携帯端末２に対応する構成要素として以下、説明するものとする。

ＣＰＵ１１（２１）は各種プログラムにしたがってこのサーバコンピュータ１（携帯端末２）の全体動作を制御する中央演算処理装置である。記憶装置１２（２２）はオペレーティングシステムや各種アプリケーションプログラム、データベース、文字フォントデータ等が予め格納されている記憶媒体１３（２３）やその駆動系を有している。この記憶媒体１３（２３）は固定的に設けたもの、もしくは着脱自在に装着可能なものであり、フロッピーディスク、ハードディスク、光ディスク、ＲＡＭカード等の磁気的・光学的記憶媒体、半導体メモリによって構成されている。また、記憶媒体内のプログラムやデータは、必要に応じてＣＰＵ１１（２１）の制御により、ＲＡＭ１４（２４）にロードされる。更に、ＣＰＵ１１（２１）は通信回線等を介して他の機器側から送信されて来たプログラム、データを受信して記憶媒体に格納したり、他の機器側に設けられている記憶媒体に格納されているプログラム、データを通信回線等を介して使用することもできる。また、ＣＰＵ１１（２１）にはその入出力周辺デバイスである入力装置１５（２５）、表示装置１６（２６）がバスラインを介して接続されており、入出力プログラムにしたがってＣＰＵ１１（２１）はそれらの動作を制御する。

【００１１】

次に、このクライアント・サーバシステムの動作を図６および図７に示すフローチャートにしたがって説明する。ここで、これらのフローチャートに記述されている各機能を実現するためのプログラムは、読み取り可能なプログラムコードの形態で記憶媒体１３（２３）に格納されており、ＣＰＵ１１（２１）はこのプログラムコードにしたがった動作を逐次実行する。なお、このことは後述する他

の実施形態についても同様である。

図６はサーバコンピュータ１側の特徴的な動作を示したフローチャートである。

先ず、アプリ・データ設定テーブル８に対してその内容を任意に設定する設定登録が指示された場合には（ステップＡ１）、アプリ・データ設定テーブル８に設定すべきＡＰソフト／データベースの名称を選択すると共に、このＡＰソフト／データベースに対してそのアクセスを許可する携帯端末２の端末名称を選択する（ステップＡ３）。すると、選択されたＡＰソフト／データベースの名称がアプリ・データ設定テーブル８に書き込まれるときに、選択された端末名称に対応する端末ＩＤを端末登録テーブル７から取得し、この端末ＩＤをＡＰソフト／データベースの名称に対応付けてアプリ・データ設定テーブル８に書き込む（ステップＡ４）。このようにして１レコード分のデータをアプリ・データ設定テーブル８に設定し終ると、設定終了が指示されたかを調べ（ステップＡ５）、設定終了が指示されるまで上述の動作が繰り返される（ステップＡ２～Ａ４）。

【００１２】

次に、ＣＦカード３への書き込みが指示された場合には（ステップＡ６）、カードリーダ／ライタ４にＣＦカード３がセットされていることを条件に（ステップＡ７）、ＣＦカード３への書き込み処理に移る。先ず、書き込みタイプの選択を行う（ステップＡ８）。ここで、ユーザは端末対応のＣＦカード３への書き込みか、端末グループ対応のＣＦカード３への書き込みかを選択指定すると、選択された書き込み形式の判別が行われる。いま、端末対応の書き込みが選択指定された場合には、カードリーダ／ライタ４にセットされているＣＦカード３から「媒体番号」を読み出し（ステップＡ９）、媒体番号対応の端末ＩＤを端末登録テーブル７から取得する（ステップＡ１０）。そして、端末ＩＤに基づいてアプリ・データ設定テーブル８を検索し、端末ＩＤ対応のＡＰソフト／データベースの名称を取得し、それに応じてＡＰソフト格納部５、データベース格納部６から該当するＡＰソフト／データベースを読み出す（ステップＡ１１）。いま、図４（Ｂ）に示すアプリ・データ設定テーブル８において、端末ＩＤが「ＩＤ１１」であれば、それに該当するＡＰソフトとして「α１」、データベースとして「Ｄ１

」がＡＰソフト格納部５、データベース格納部６から読み出される。

【００１３】

このようにして取得した端末ＩＤ対応のＡＰソフト／データベースをそのＣＦカード３へ書き込むと共に（ステップＡ１２）、上述のステップＡ１０で取得した端末ＩＤをそのＡＰソフト／データベースに対するアクセス制御情報として書き込む（ステップＡ１３）。このような書き込みが終ると、その端末ＩＤに対応してアプリ・データ設定テーブル８に書き込み済であることを示す「書き込みフラグ」をセットする（ステップＡ１４）。そして、カードリーダ／ライタ４に複数枚のＣＦカード３がセットされてる場合、未書き込みのＣＦカード３が有るかを調べ（ステップＡ１５）、有ればステップＡ９に戻り、次のＣＦカード３をアクセスしてその「媒体番号」を読み出し、そのＣＦカード３に対して上述と同様の書き込み処理を行う。これによってセット中の全てのＣＦカード３に対してその書き込みが終ると、アプリ・データ設定テーブル８を参照し、「書き込みフラグ」がセットされていない端末ＩＤを抽出し、この端末ＩＤに該当する端末名称を端末登録テーブル７から取得し、未書き込み端末名称として一覧表示させると共に（ステップＡ１６）、書き込み完了メッセージを表示出力させる（ステップＡ１７）。

【００１４】

一方、端末グループ対応のＣＦカード３に対応する書き込みが選択指定された場合には、端末グループ名の選択画面が表示され、その中から所望のグループ名を選択指定すると（ステップＡ１８）、このグループ名に基づいてグループ登録テーブル９を検索し、該当する複数の端末ＩＤを取得する（ステップＡ１９）。そして、この複数の端末ＩＤに基づいてアプリ・データ設定テーブル８の内容をその先頭から検索し、その端末ＩＤが１つでも含まれていれば、それに対応するＡＰソフト／データベースをＡＰソフト格納部５、データベース格納部６から読み出す（ステップＡ２０）。ここで、端末グループＡが選択された場合には、ＡＰソフト「α１」を取得する。そして、取得したＡＰソフト／データベースをそれに対応する端末ＩＤと共にＣＦカード３に書き込む（ステップＡ２１、Ａ２２）。この場合、ＡＰソフト「α１」と端末ＩＤ「ＩＤ１１」、「ＩＤ１２」とが

対応付けられてＣＦカード３に書き込まれる。そして、カードリーダ／ライタ４にセットされている全てのＣＦカード３に対して同様の書き込みが終了するまで柔術の動作が繰り返される（ステップＡ２１～Ａ２３）。これによって全媒体への書き込みが終ると、ステップＡ２４に進み、同一グループ内において未書き込みのＡＰソフト／データベースがアプリ・データ設定テーブル８内にまだ有るかを調べ、有ればステップＡ２０に戻るため、次に、端末グループＡに該当するＡＰソフトとして「α２」が読み出され、端末ＩＤ「ＩＤ１３」と共に各ＣＦカード３に書き込まれる。以下、同様に、データベース「Ｄ１」、端末ＩＤ「ＩＤ１１」が各ＣＦカード３に書き込まれ、次でデータベース「Ｄ２」、端末ＩＤ「ＩＤ１２」、更にデータベース「Ｄ３」、端末ＩＤ「ＩＤ１３」が各ＣＦカード３に書き込まれる。この結果、端末グループＡ対応の各ＣＦカード３の内容は、図２（Ｂ）に示す如くとなり、端末グループＡ対応の書き込みが全て完了すると、書き込み完了メッセージが表示される（ステップＡ１７）。このようにしてＡＰソフト／データベースの書き込みが行われたＣＦカード３は、対応する携帯端末２側へそれぞれ配布される。

【００１５】

図７は携帯端末２側の動作を示したフローチャートであり、電源投入に伴って実行開始される。先ず、初期メニュー画面の中から任意のＡＰソフト／データベースが選択されてその起動アクセスが指示された場合に（ステップＢ１）、その携帯端末２にＣＦカード３がセットされていなければ（ステップＢ２）、その起動アクセスを無効とするためにステップＢ１に戻るが、ＣＦカード３がセットされていれば、予め設定されている自己の端末ＩＤを読み出す（ステップＢ３）。そして、ＣＦカード３をアクセスしてそれに格納されている端末ＩＤを読み出し（ステップＢ４）、自己の端末ＩＤと一致するかを調べる（ステップＢ５）。この場合、グループ対応のＣＦカード３にはＡＰソフト／データベース毎にそのグループに属する他の端末ＩＤも格納されているので、選択指定されたＡＰソフト／データベースに対応する端末ＩＤをＣＦカード３から読み出し、その中に自己の端末ＩＤが含まれているかを調べる。ここで、端末ＩＤの一致が検出された場合にはそれを条件に選択指定されたＡＰソフト／データベースのアクセスが許可

され、それに応じた処理の実行に移行するが（ステップＢ６）、端末ＩＤの不一致が検出された場合にはステップＢ１に戻るため、そのＡＰソフト／データベースのアクセスは禁止される。

【００１６】

以上のようにこの第１実施形態において、ＣＦカード３内のＡＰソフト／データベースをアクセスしてデータ処理を行う際に、携帯端末２はＣＦカード３から読み込んだ端末ＩＤと予め設定されている自己の端末ＩＤとを比較し、その一致／不一致によってＣＦカード３内のＡＰソフト／データベースに対するアクセスが制御されるので、特定の携帯端末２に対してのみＣＦカード３内のＡＰソフト／データベースをアクセスすることが可能となる。つまり、ＣＦカード３内のＡＰソフト／データベースをアクセスすることができる携帯端末２を制限するようにしたから、端末毎のアクセス制御が可能となると共に、アクセス権限を有しない他の携帯端末２による不法なコピー複製を効果的に禁止することができる。

このことは端末対応のＣＦカード３に限らず、グループ対応のＣＦカード３についても同様であり、営業地域毎に特定のＡＰソフト／データベースを使用する場合、地域毎に端末グループを分けておけば、端末グループ毎のアクセス制御が可能となる。またＣＦカード３内に個々のＡＰソフト／データベースに対応付けて端末ＩＤが格納されている場合には、端末毎、ＡＰソフト／データベース毎にそのアクセス制御が可能となる。すなわち、ＣＦカード３内に複数のＡＰソフト／データベースが格納されている場合、特定のＡＰソフト／データベースに対してはアクセスが許可されるが、他のＡＰソフト／データベースについてはそのアクセスを禁止することができ、同一の端末グループに属する携帯端末２であっても、ＡＰソフト／データベース毎にそのアクセスを制御することが可能となる。

【００１７】

一方、サーバコンピュータ１はＣＦカード３内のＡＰソフト／データベースを書き込むことによりこのＣＦカード３を介して携帯端末２側にＡＰソフト／データベースを配布するが、その際、サーバコンピュータ１はこのＣＦカード３に対応付けられている端末ＩＤを読み出してＣＦカード３内にＡＰソフト／データベースと共にこの端末ＩＤを書き込むようにしたから、ＡＰソフト／データベース

のアクセスを許可する携帯端末２を特定することができる。これによって端末毎のアクセス制御が可能となると共に、アクセス権限を有しない他の携帯端末２による不法なコピー複製を効果的に禁止することができる。また、サーバコンピュータ１は個々のＡＰソフト／データベース毎にそのアクセスを許可する端末を定義するアプリ・データ設定テーブル８を参照することによって端末対応のＣＦカード３毎に、書き込み対象のＡＰソフト／データベースを特定することができる。

このことは、端末対応のＣＦカード３に限らず、グループ対応のＣＦカード３についても同様であり、同じ端末グループに属する各携帯端末２の端末ＩＤをＣＦカード３内に書き込むことで、ＡＰソフト／データベースのアクセスを許可する端末グループを特定することができ、これによって端末グループ毎のアクセス制御が可能となる。

【００１８】

なお、上述した第１実施形態は持ち運び自在な記憶媒体としてＣＦカードを示したが、これに限らず、磁気的、光学的記録媒体、半導体メモリ等、任意であり、またカード型に限らず、カートリッジ型のディスク等であってもよい。また、クライアント端末はモバイル型の携帯端末２に限らず、ディスクトップ型の端末であってもよい。更に、記録媒体内のＡＰソフト／データベースに対応してそのアクセスを許可する端末ＩＤを書き込む場合に限らず、そのアクセスを禁止する端末ＩＤを書き込むようにしてもよい。

【００１９】

（第２実施形態）

以下、図８～図１０を参照してこの発明の第２実施形態を説明する。なお、上述した第１実施形態においては、持ち運び自由な可搬型の記憶媒体を介してサーバコンピュータ１と携帯端末２との間でデータの授受を行うオフライン型のクライアント・サーバシステムを示したが、この第２実施形態は複数台のクライアント端末がネットワークを介してサーバコンピュータに通信接続されて成るオンライン型のクライアント・サーバシステムに適用したもので、基本的には第１実施形態と同様の構成となっている。

【００２０】

図８はこの第２実施形態におけるクライアント・サーバシステムを示したシステム構成図であり、このクライアント・サーバシステムはサーバコンピュータ３１に専用回線あるいは公衆回線を介して複数台のクライアント端末３２が接続されたローカルエリアネットワークあるいは広域ネットワークシステムである。このサーバコンピュータ３１側には端末登録テーブル３３、アプリ・データ設定テーブル３４が設けられている。この端末登録テーブル３３、アプリ・データ設定テーブル３４は上述した第１実施形態で示した端末登録テーブル７、アプリ・デー設定テーブル８（図４（Ａ）、（Ｂ）参照）と基本的に同様の構成で、端末登録テーブル３３は「端末名称」、「端末ＩＤ」とを対応付けた構成となっている。また、アプリ・データ設定テーブル３４はＡＰソフト／データベース毎にそのアクセスを許可する端末を識別するための端末ＩＤを対応付けて記憶するもので、各ＡＰソフト／データベースに対応付けて１または２以上の端末ＩＤが記憶されている。ここで、クライアント端末３２側からＡＰソフト／データベースの送信要求が有った際に、サーバコンピュータ３１は端末登録テーブル３３、アプリ・データ設定テーブル３４を参照し、要求されたＡＰソフト／データベースに対してそのアクセスが許可されている端末からの要求であれば、それを条件に、ＡＰソフト／データベースを要求元へ送信するようにしている。

【００２１】

次に、この第２実施形態の動作を図９、図１０に示すフローチャートにしたがって説明する。図９はクライアント端末３２側の動作を示し、図１０はサーバコンピュータ３１側の動作を示したフローチャートである。

先ず、クライアント端末３２側において、自己の端末ＩＤをサーバコンピュータ３１側の端末登録テーブル３３に登録すべきＩＤ登録が指示された場合には（ステップＣ１）、自己の端末名称を入力したのち（ステップＣ２）、予め設定されている自己の端末ＩＤを読み出し（ステップＣ３）、サーバコンピュータ３１に対してＩＤ登録を要求し、ＯＫ応答（肯定応答）が有るまでＩＤ登録を要求し続ける（ステップＣ４、Ｃ５）。ここで、ＯＫ応答が有れば、端末ＩＤをサーバコンピュータ３１へ送信する（ステップＣ６）ここで、サーバコンピュータ３１

側においては、端末側からの要求がＩＤ登録であれば（ステップＤ２～Ｄ４）、その要求を正常に受信したことを示すために要求元へＯＫ応答を返信し（ステップＤ１６）、これによってクライアント端末３２側から送信されて来る端末名称、端末ＩＤを受信すると（ステップＤ１７）、それが予め決められている書式通りのデータであれば（ステップＤ１８）、端末登録テーブル３３にこの端末名称と端末ＩＤとを対応付けて登録する（ステップＤ１９）。そして、正常登録した旨を示すために、要求元へＯＫ応答を行う（ステップＤ２０）。一方、端末から送信されて来た端末名称、端末ＩＤが書式通りのデータでなければ、要求元に対してエラー応答を行う（ステップＤ１５）。これによってクライアント端末３２側ではサーバコンピュータ３１からの応答がＯＫ応答であれば（ステップＣ７）、登録終了メッセージを表示させるが（ステップＣ８）、エラー応答であればエラーメッセージを表示させる（ステップＣ９）。

【００２２】

このようにサーバコンピュータ３１は各クライアント端末３２からＩＤ登録が要求される毎に、端末名称、端末ＩＤとを対応付けて端末登録テーブル３３に順次登録してゆく。一方、サーバコンピュータ３１側において、ＡＰソフト／データベースに対するアクセスをどの端末に許可するかをＡＰソフト／データベース毎に設定するために、その設定を指示すると、上述した第１実施形態と同様の処理（図６のステップＡ１～Ａ５）によってアプリ・データ設定テーブル３４が作成される（ステップＤ１、Ｄ５～Ｄ８）。このようにサーバコンピュータ３１側に端末登録テーブル３３、アプリ・データ設定テーブル３４が作成されている状態で、クライアント端末３２側でＡＰソフト／データベースの送信要求を指示すると（図１０のステップＣ１０）、予め設定されている自己の端末ＩＤを読み出し（ステップＣ１１）、サーバコンピュータ３１に対してＡＰソフト／データベースの送信要求を行いＯＫ応答が有るまで要求し続け（ステップＣ１２、Ｃ１３）、ＯＫ応答が有れば端末ＩＤを送信する（ステップＣ１４）。

【００２３】

一方、サーバコンピュータ３１側においては、クライアント端末３２からの要求がＡＰソフト／データベースの送信要求であれば（ステップＤ２、Ｄ３）、要

求元へＯＫ応答を送信したのち（ステップＤ９）、端末ＩＤの受信待ちとなり、要求元からの端末ＩＤを受信すると（ステップＤ１０）、受信した端末ＩＤに基づいて端末登録テーブル３３を検索し、予め登録されている正規の端末からの要求であるかを調べる（ステップＤ１１）。ここで、正規の端末からの要求でなければ、その要求元へエラー応答を行うが（ステップＤ１５）、正規の端末からの要求であれば、要求元へＯＫ応答を行うと共に（ステップＤ１２）、その端末ＩＤに基づいてアプリ・データ設定テーブル３４を検索し、端末ＩＤ対応のＡＰソフト／データベースを選択的に読み出して要求元へ送信する（ステップＤ１３、Ｄ１４）。この場合、端末ＩＤ対応のＡＰソフト／データベースが複数存在していれば、その全てを要求元へ送信するようにしてもよいが、所望のＡＰソフト／データベースのみの送信要求があれば、要求されたＡＰソフト／データベースだけを送信する。

すると、クライアント端末３２側においては、サーバコンピュータ３１からエラー応答が有れば（ステップＣ１５）、エラーメッセージを表示出力させるが（ステップＣ９）、ＯＫ応答が有れば（ステップＣ１５）、サーバコンピュータ３１側から通信されて来たＡＰソフト／データベースを受信して登録保存する（ステップＣ１６、Ｃ１７）。そして、このＡＰソフト／データベースを起動させてデータ処理を開始する（ステップＣ１８）。なお、サーバコンピュータ３１からのＡＰソフト／データベースが登録保存されている状態においては、その起動指示に応じていつでも自由にＡＰソフト／データベースにしたがったデータ処理を実行することができる（ステップＣ１９、Ｃ１８）。

【００２４】

以上のようにこの第２実施形態におけるオンライン型のクライアント・サーバシステムにおいては、いずれかのクライアント端末３２からＡＰソフト／データベースに対するアクセス要求があった際に、要求元のクライアント端末３２から送信されて来た端末ＩＤと、アプリ・データ設定テーブル３４内のＡＰソフト／データベースに対応する端末ＩＤとを比較し、その比較結果に応じてＡＰソフト／データベースに対するアクセス可否を決定するようにしたから、特定端末に対してのみＡＰソフト／データベースのアクセスを許可することで、不法なＡＰソ

フト／データベースのダウンロードを禁止し、そのセキュリティを維持することが可能となる。

【００２５】

なお、上述した第２実施形態においては、端末登録テーブル３３を設けたが、アプリ・データ設定テーブル３４だけ設ける構成としてもよい。また、ＡＰソフト／データベースの送信要求に応じてＡＰソフト／データベースを要求元へ送信するようにしたが、クライアント端末３２がサーバコンピュータ３１内のＡＰソフト／データベースを直接アクセスするようにしてもよい。またオンライン型システムに限らず、無線通信や光通信を媒体とするシステムであってもよい。

また、上述した各実施形態において、端末ＩＤの構成は任意であり、端末製造時の製造番号、例えば、「国コード＋製造会社コード＋機能コード＋端末シリアル番号」であってもよい。また公衆電話回線をネットワークとするシステムにおいては、「国電話コード＋地域電話コード＋電話番号」であってもよい。

更に、ＡＰソフト／データベースと端末ＩＤとを対応付けたテーブルに限らず、ＡＰソフト／データベース毎にそのアクセスを許可する端末あるいはそのアクセスを禁止する端末を論理条件式で記述したテーブルとしてもよい。例えば、等号、不等号を用いて端末ＩＤの番号が所定範囲内にあればアクセス可あるいは不可を定義するようにしてもよい。

【００２６】

【発明の効果】

第１の発明によれば、アプリケーションソフト／データが格納されている記録媒体をアクセスしてデータ処理を行うデータ処理装置において、特定のデータ処理装置に対してのみ記録媒体内のアプリケーションソフト／データのアクセスを許可することで、装置毎のアクセス制御が可能となり、セキュリティ維持と共にアクセス権限を有しない他の装置による不法なコピー複製を効果的に禁止することができる。

第２の発明によれば、アプリケーションソフト／データを記録媒体に書き込んで各端末に配布するデータ処理装置において、特定端末に対してのみアプリケーションソフト／データのアクセスを許可／禁止するための書き込みを行うことで

、端末毎のアクセス制御が可能となりセキュリティ維持と共に、アクセス権限を有しない他の端末による不法なコピー複製を効果的に禁止することができる。

第３の発明は、端末装置との間でネットワークを介してデータ通信を行うデータ処理装置において、特定端末に対してのみアプリケーションソフト／データのアクセスを許可することで、不法なアプリケーションソフト／データのダウンロードを禁止し、そのセキュリティを維持することができる。

【図面の簡単な説明】

【図１】

オフライン型のクライアント・サーバシステムを示したシステム構成図。

【図２】

（Ａ）端末対応のＣＦカード３内のデータを示した図、（Ｂ）は端末グループＡ対応のＣＦカード３内のデータを示した図、（Ｃ）は端末グループＢ対応のＣＦカード３内のデータを示した図。

【図３】

端末グループＡ、端末グループＢを説明するための図。

【図４】

（Ａ）は端末登録テーブル７のデータ構造を示した図、（Ｂ）はアプリ・データ設定テーブル８のデータ構造を示した図、（Ｃ）はグループ登録テーブル９のデータ構造を示した図。

【図５】

サーバコンピュータ１（携帯端末２）の全体構成を示したブロック図。

【図６】

サーバコンピュータ１側の特徴的な動作を示したフローチャート。

【図７】

携帯端末２側の特徴的な動作を示したフローチャート。

【図８】

第２実施形態におけるオンライン型クライアント・サーバシステムを示したシステム構成図。

【図９】

第２実施形態においてクライアント端末３２側の動作を示したフローチャート。

【図１０】

第２実施形態においてサーバコンピュータ３１側の動作を示したフローチャート。

【符号の説明】

１、３１　サーバコンピュータ

２　携帯端末

３　ＣＦカード

４　カードリーダ／ライタ

５　ＡＰソフト格納部

６　データベース格納部

７、３３　端末登録テーブル

８、３４　アプリ・データ設定テーブル

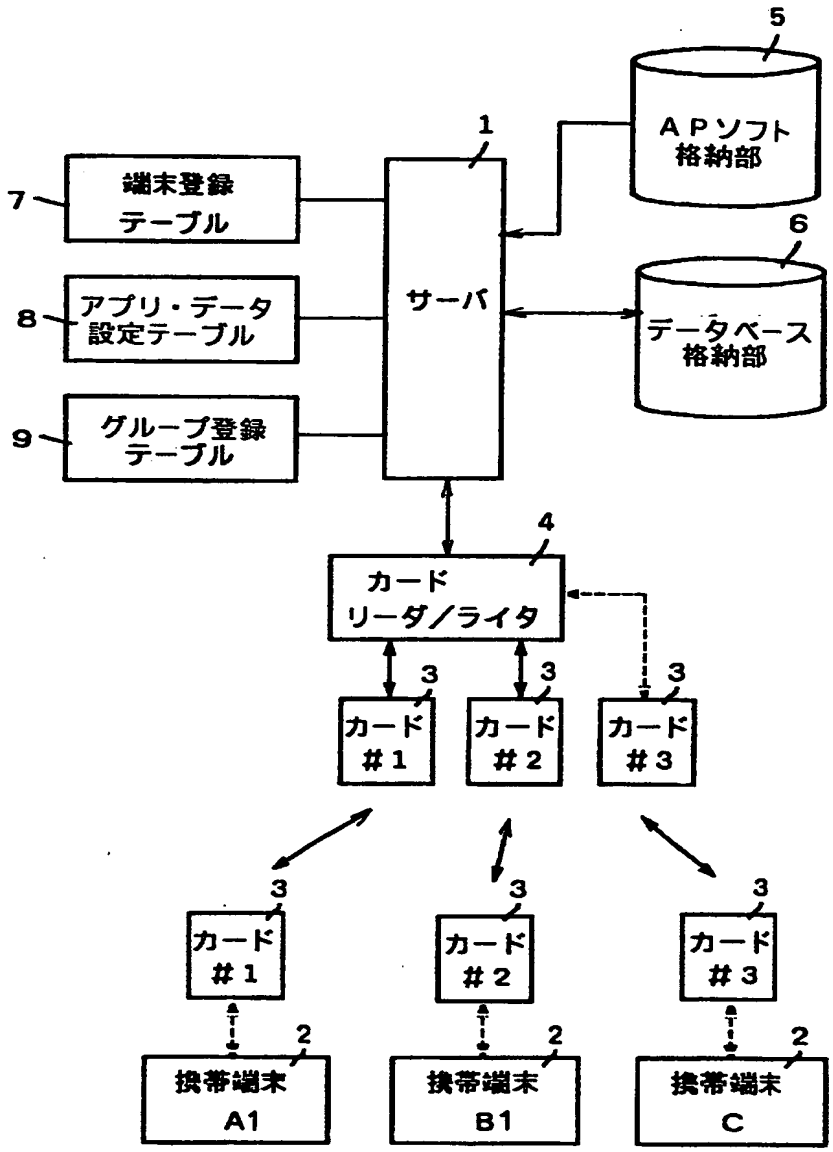
９　グループ登録テーブル

３２　クライアント端末

Ａ、Ｂ　端末グループ

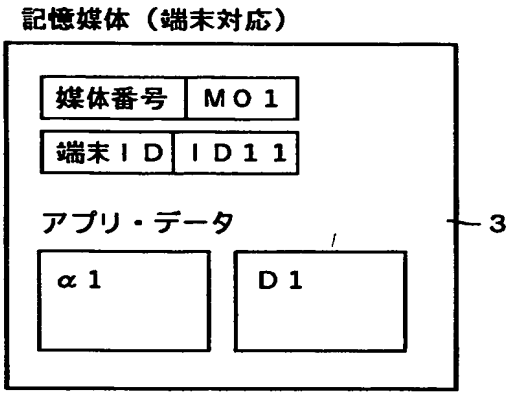
【書類名】　　図面

【図１】

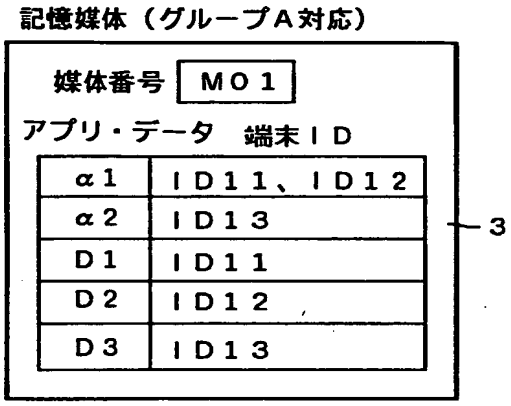

5
APソフト
格納部
1
7
端末登録
テーブル
6
サーバ
データベース
格納部
8
アプリ・データ
設定テーブル
9
グループ登録
テーブル
4
カード
リーダ/ライタ
3
カード
#1
3
カード
#2
3
カード
#3
3
カード
#1
3
カード
#2
3
カード
#3
2
携帯端末
A1
2
携帯端末
B1
2
携帯端末
C

【図２】

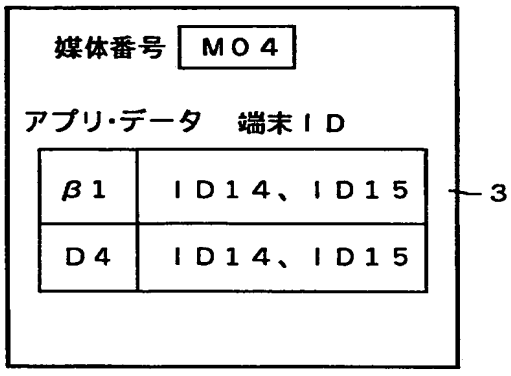
(A)



(B)

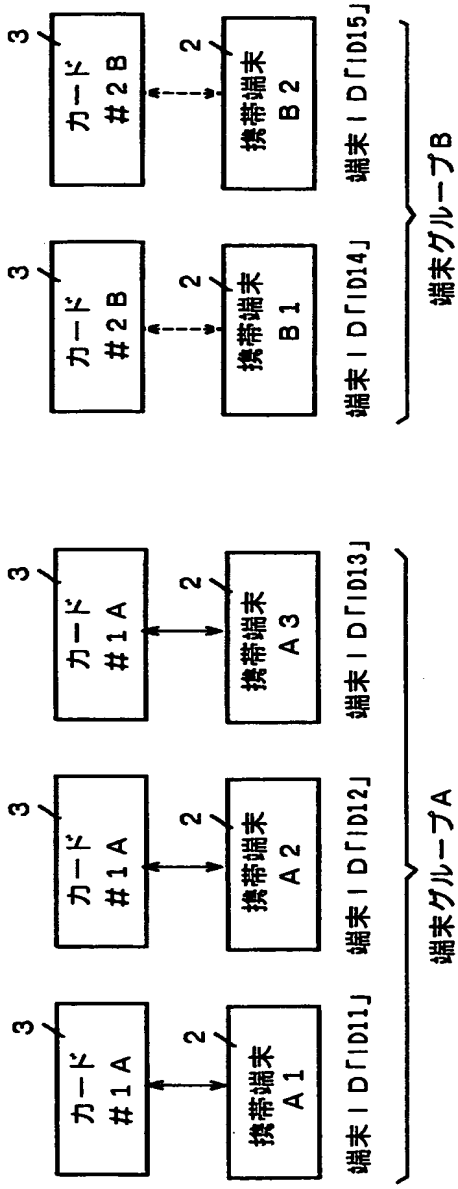


(C)

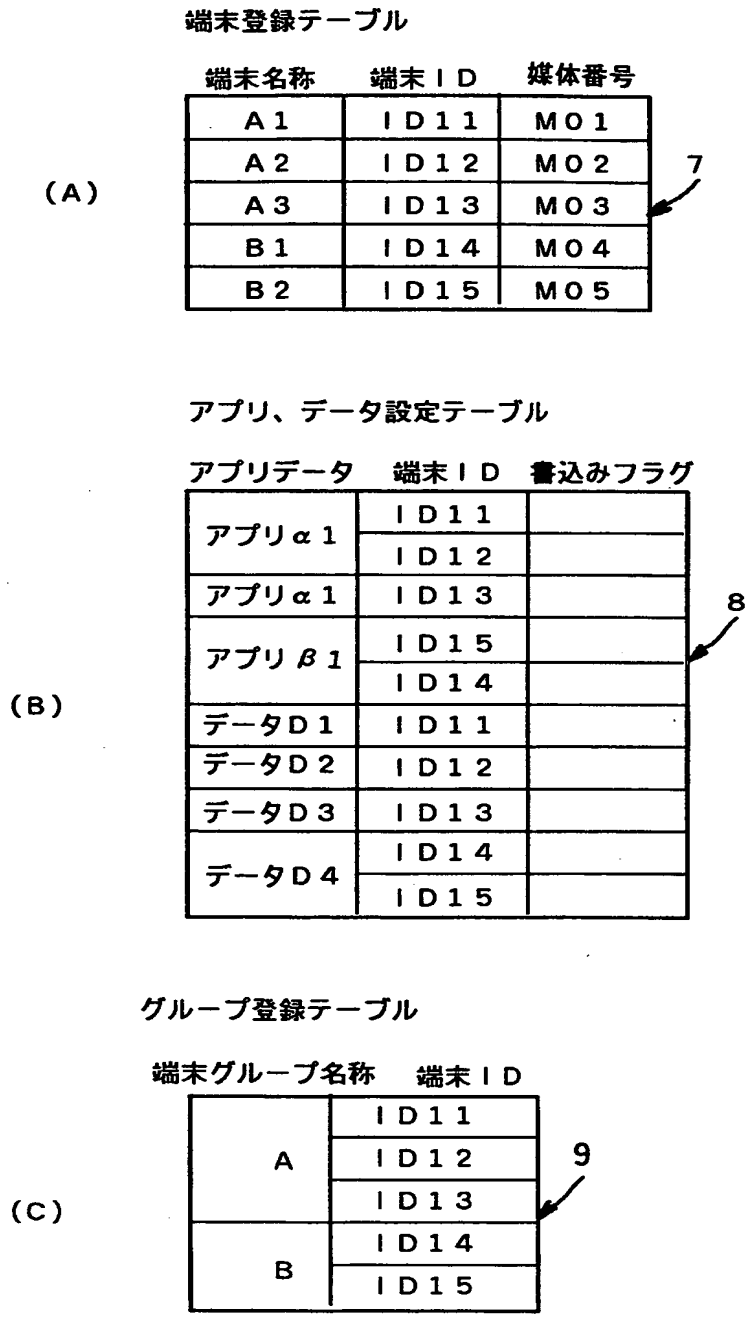


出証特２０００－３００９９７２

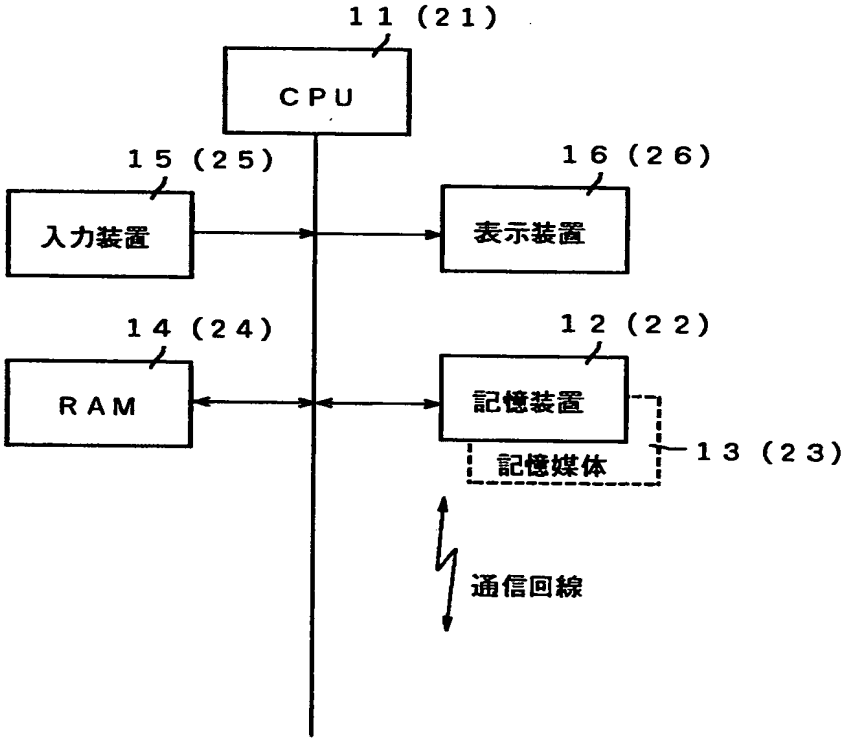
【図３】


3
カード
＃１Ａ
2
携帯端末
Ａ１
端末ＩＤ「ID11」
3
カード
＃１Ａ
2
携帯端末
Ａ２
端末ＩＤ「ID12」
3
カード
＃１Ａ
2
携帯端末
Ａ３
端末ＩＤ「ID13」
端末グループＡ
3
カード
＃２Ｂ
2
携帯端末
Ｂ１
端末ＩＤ「ID14」
3
カード
＃２Ｂ
2
携帯端末
Ｂ２
端末ＩＤ「ID15」
端末グループＢ

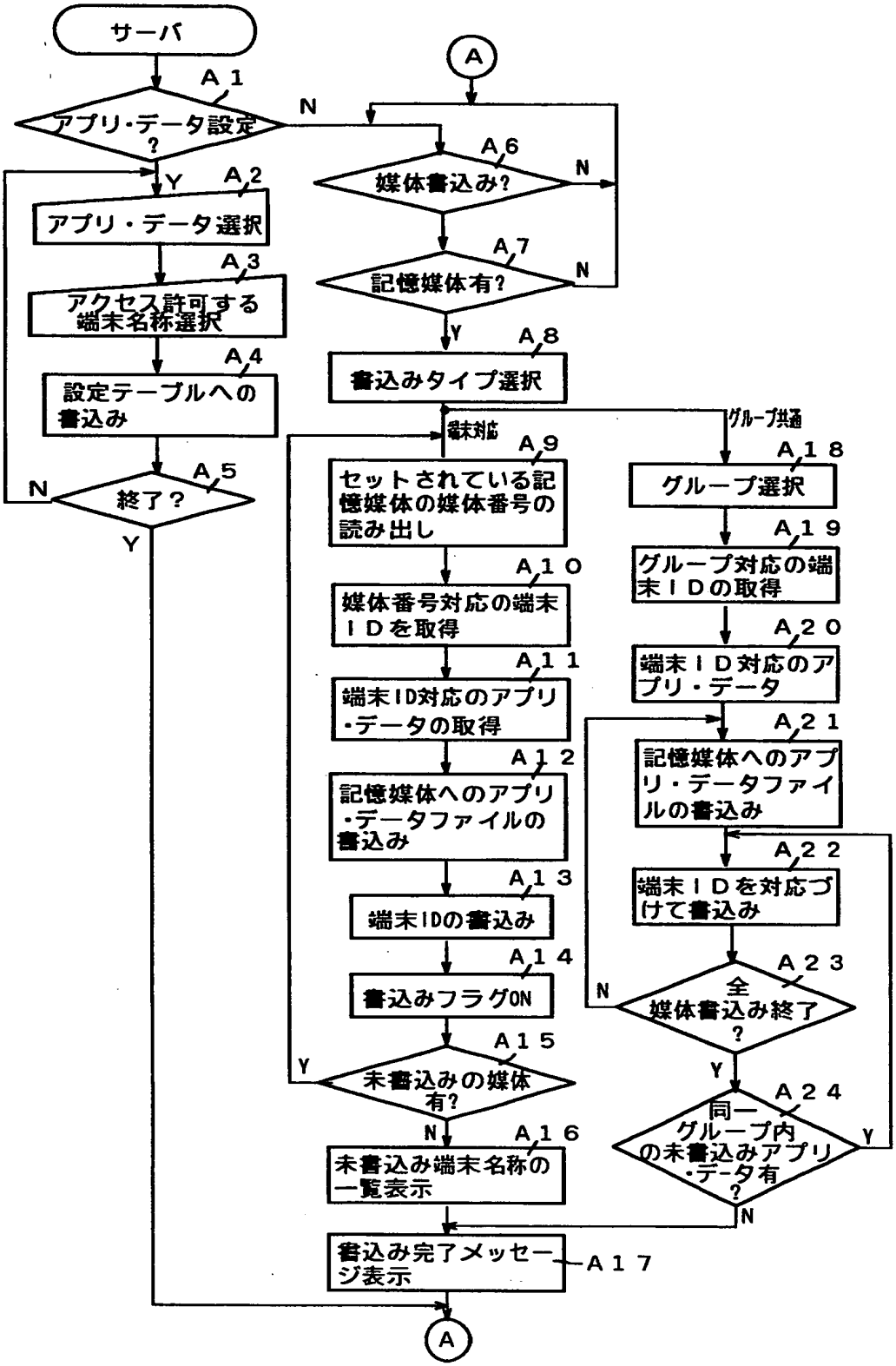
【図４】


端末登録テーブル
端末名称
端末ＩＤ
媒体番号
Ａ１
ＩＤ１１
Ｍ０１
Ａ２
ＩＤ１２
Ｍ０２
Ａ３
ＩＤ１３
Ｍ０３
Ｂ１
ＩＤ１４
Ｍ０４
Ｂ２
ＩＤ１５
Ｍ０５
７
（Ａ）
アプリ、データ設定テーブル
アプリデータ
端末ＩＤ
書込みフラグ
アプリα１
ＩＤ１１
ＩＤ１２
アプリα１
ＩＤ１３
アプリβ１
ＩＤ１５
ＩＤ１４
８
（Ｂ）
データＤ１
ＩＤ１１
データＤ２
ＩＤ１２
データＤ３
ＩＤ１３
データＤ４
ＩＤ１４
ＩＤ１５
グループ登録テーブル
端末グループ名称
端末ＩＤ
Ａ
ＩＤ１１
ＩＤ１２
ＩＤ１３
９
（Ｃ）
Ｂ
ＩＤ１４
ＩＤ１５

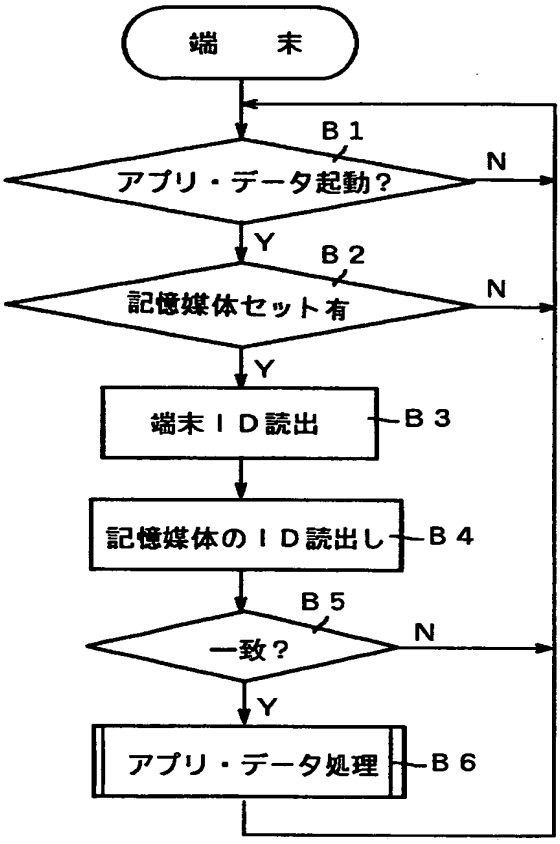
【図５】


１１（２１）
CPU
１５（２５）
入力装置
１６（２６）
表示装置
１４（２４）
RAM
１２（２２）
記憶装置
１３（２３）
記憶媒体
通信回線

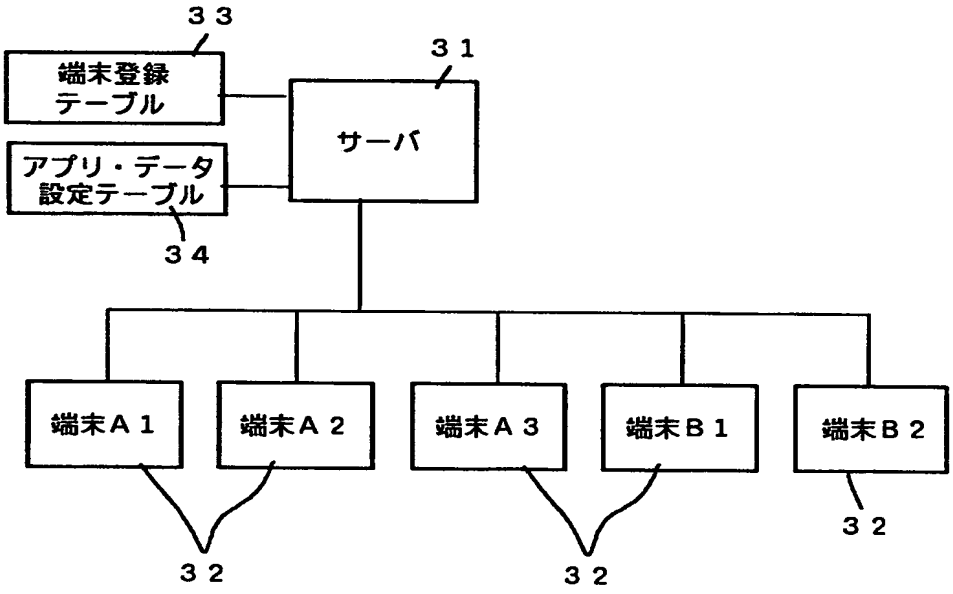
【図６】


サーバ
A1
アプリ･データ設定?
N
Y
A2
アプリ・データ選択
A3
アクセス許可する端末名称選択
A4
設定テーブルへの書込み
A5
終了?
N
Y
A
A6
媒体書込み?
N
A7
記憶媒体有?
N
Y
A8
書込みタイプ選択
端末対応
グループ共通
A9
セットされている記憶媒体の媒体番号の読み出し
A10
媒体番号対応の端末ＩＤを取得
A11
端末ID対応のアプリ・データの取得
A12
記憶媒体へのアプリ・データファイルの書込み
A13
端末IDの書込み
A14
書込みフラグON
A15
未書込みの媒体有?
Y
N
A16
未書込み端末名称の一覧表示
A17
書込み完了メッセージ表示
A
A18
グループ選択
A19
グループ対応の端末ＩＤの取得
A20
端末ＩＤ対応のアプリ・データ
A21
記憶媒体へのアプリ・データファイルの書込み
A22
端末ＩＤを対応づけて書込み
A23
全媒体書込み終了?
N
Y
A24
同一グループ内の未書込みアプリ・データ有?
Y
N

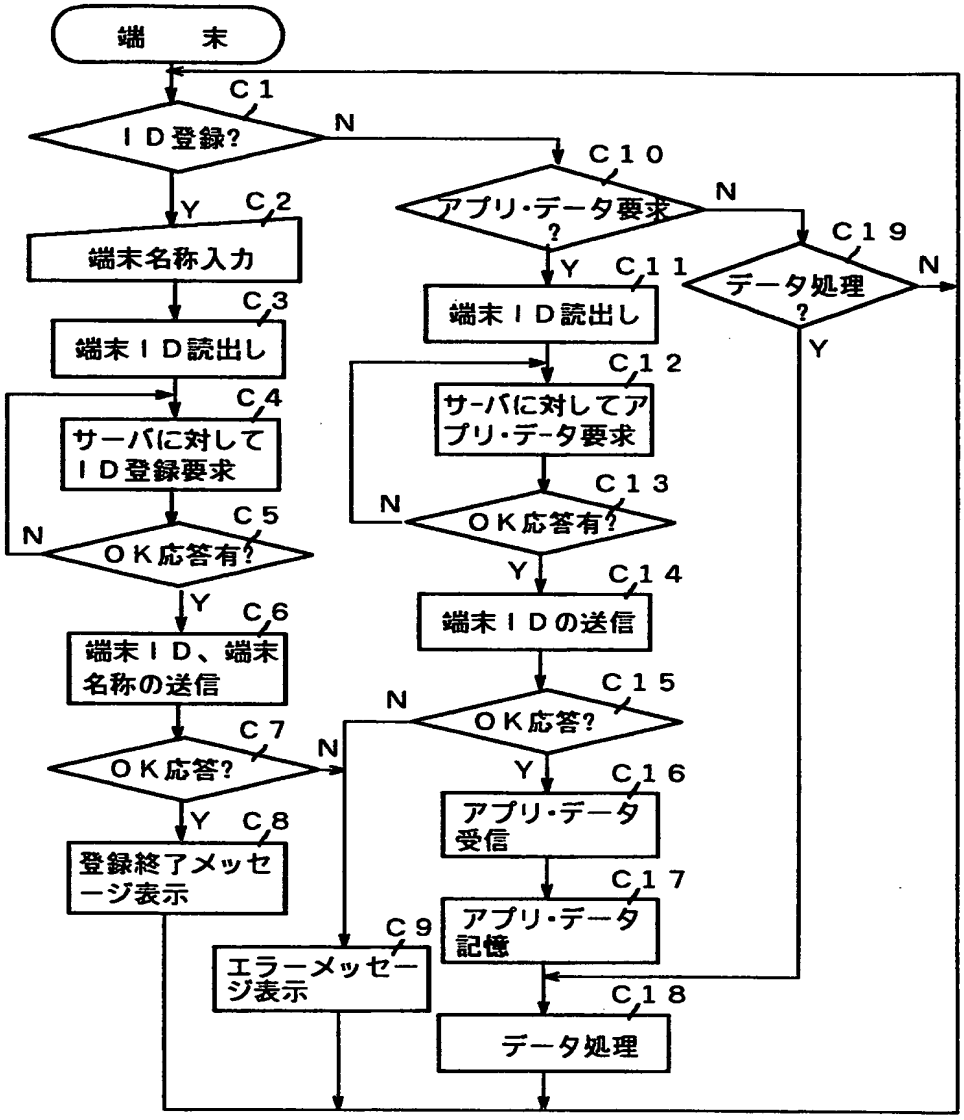
【図７】


端　末
B１
アプリ・データ起動？
N
Y
B２
記憶媒体セット有
N
Y
端末ＩＤ読出
B３
記憶媒体のＩＤ読出し
B４
B５
一致？
N
Y
アプリ・データ処理
B６

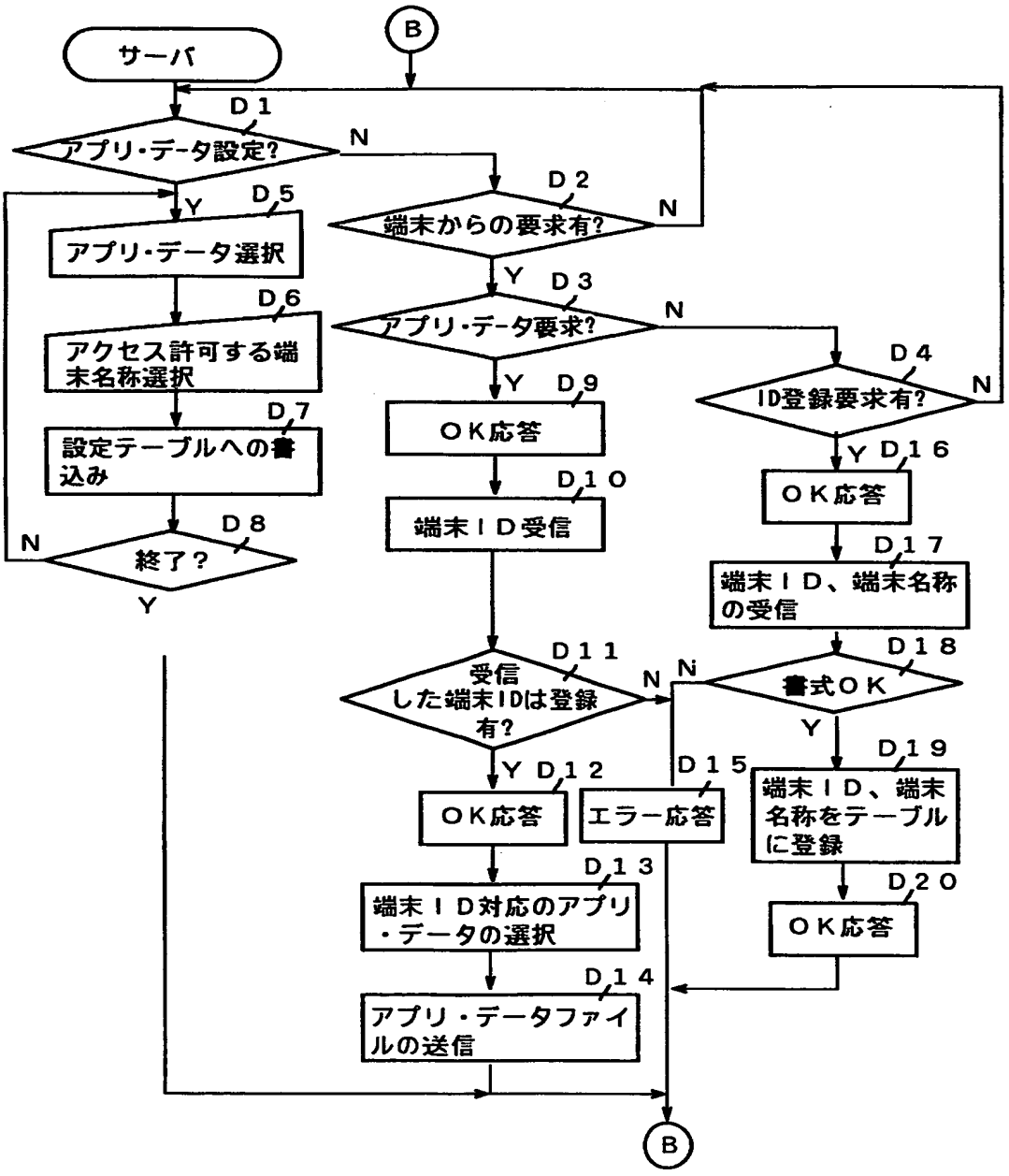
【図８】


３３
３１
端末登録
テーブル
サーバ
アプリ・データ
設定テーブル
３４
端末Ａ１
端末Ａ２
端末Ａ３
端末Ｂ１
端末Ｂ２
３２
３２
３２

【図９】


端　末
C1
ＩＤ登録?
N
Y
C2
端末名称入力
C3
端末ＩＤ読出し
C4
サーバに対して
ＩＤ登録要求
C5
ＯＫ応答有?
N
Y
C6
端末ＩＤ、端末
名称の送信
C7
ＯＫ応答?
N
Y
C8
登録終了メッセ
ージ表示
C9
エラーメッセー
ジ表示
C10
アプリ・データ要求
?
N
Y
C11
端末ＩＤ読出し
C12
サーバに対してア
プリ・データ要求
C13
ＯＫ応答有?
N
Y
C14
端末ＩＤの送信
C15
ＯＫ応答?
N
Y
C16
アプリ・データ
受信
C17
アプリ・データ
記憶
C18
データ処理
C19
データ処理
?
N
Y

【図１０】


サーバ
B
D１
アプリ・データ設定?
N
Y
D２
端末からの要求有?
N
Y
D３
アプリ・データ要求?
N
Y
D４
ID登録要求有?
N
Y
D５
アプリ・データ選択
D６
アクセス許可する端末名称選択
D７
設定テーブルへの書込み
D８
終了?
N
Y
D９
ＯＫ応答
D１０
端末ＩＤ受信
D１１
受信した端末IDは登録有?
N
Y
D１２
ＯＫ応答
D１３
端末ＩＤ対応のアプリ・データの選択
D１４
アプリ・データファイルの送信
D１５
エラー応答
D１６
ＯＫ応答
D１７
端末ＩＤ、端末名称の受信
D１８
書式ＯＫ
N
Y
D１９
端末ＩＤ、端末名称をテーブルに登録
D２０
ＯＫ応答
B

【書類名】　　要約書

【要約】

【課題】　アプリケーションソフト／データが格納されている記録媒体をアクセスしてデータ処理を行うデータ処理装置において、特定のデータ処理装置に対してのみ記録媒体内のアプリケーションソフト／データのアクセスを許可することで、装置毎のアクセス制御が可能となり、セキュリティ維持と共にアクセス権限を有しない他の装置による不法なコピー複製を効果的に禁止する。

【解決手段】　ＡＰソフト／データベースが格納されている持ち運び自在なＣＦカード３がセットされている状態で、このＣＦカード３内のＡＰソフト／データベースをアクセスしてデータ処理を行う携帯端末２において、携帯端末２はＣＦカード３内に予め格納されている端末ＩＤを読み込む。そして、このＣＦカード３内の端末ＩＤと予め設定されている自己の端末ＩＤとを比較し、その比較結果に基づいてＣＦカード３内のＡＰソフト／データベースに対するアクセス可否を決定する。

【選択図】　　図１

認定・付加情報

特許出願の番号	平成１１年　特許願　第１２１２００号
受付番号	５９９００４１０９９４
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１１年　６月　２日

＜認定情報・付加情報＞

【提出日】　平成11年 4月28日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００１４４３〕

１．変更年月日　　１９９８年　１月　９日
［変更理由］　住所変更
住　所　　東京都渋谷区本町１丁目６番２号
氏　名　　カシオ計算機株式会社